DEPARTMENT OF THE ARMY
HEADQUARTERS, U.S. ARMY MEDICAL DEPARTMENT CENTER AND SCHOOL
AND FORT SAM HOUSTON
2250 STANLEY ROAD
FORT SAM HOUSTON, TEXAS 78234-6100

REPLY TO
ATTENTION OF

IMSW-SMH-IM

11 JUL 2006

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Installation Information Management (IM) Policy 25-12, Removal of Unauthorized Software or Data from Computers

1. REFERENCE. The following are the baseline references used to establish this local policy.

a. AR 25-1, Army Knowledge Management and Information Technology Management, 15 July 2005.

b. AR 25-2, Information Assurance, 14 November 2003.

2. PURPOSE. To establish policy and procedures for removing unauthorized software or data from computers.

3. SCOPE. This policy applies to all organizations and units located on or supported by Fort Sam Houston (FSH), Camp Bullis, and Camp Stanley, and that have connectivity to the installation network managed by the Director of Information Management (DOIM). This policy applies to Government-owned and leased automation equipment, and any Designated Approval Authority (DAA) authorized system, or unauthorized/illegally equipment connected to the Fort Sam Houston Network.

4. POLICY.

a. Per AR 25-1, users will not install new software packages, software upgrades, free software, freeware, shareware, and so on, without the authorization of their IAM, Configuration Control Board, and DAA. Unauthorized software may contain harmful viruses or defects, which can result in the loss of data or system failure. Additionally, the use of such software may create configuration management problems, violate software copyrights or licensing agreements, or cause other difficulties.

b. The DOIM has the responsibility to scan all computers and to monitor Internet traffic to ensure individual activity is in keeping with regulatory compliance and the required level of professionalism for military, civilian, and contract personnel at FSH. System and Network scanning will be accomplished by properly trained and designated IA personnel using Army Approved tools.

c. Any computer identified with unlicensed software (including shareware or freeware), inappropriate material, or questionable Internet history will be evaluated by the DOIM to determine the level of sanitation required to return the equipment to an acceptable level.

d. AR 25-2 requires IA personnel remove or block any unnecessary or unauthorized services, software, and applications (for example, gaming software, Gnutella, IRC, ICQ, Instant Messaging, peer-to-peer). All unauthorized software and/or data encountered during scans, must be removed by designated DOIM technicians with appropriate Information Assurance credentials. This may require relocation of the hardware to DOIM facilities. Relocation of hardware will be coordinated with appropriate hand receipt holder to insure property accountability records are maintained.

e. Fort Sam Houston IA Personnel designated to remove unauthorized applications, services and software are; System Administrators, Network Administrators, Help Desk Technicians, Information Assurance Security Officers (IASO), and Information Assurance Network Officers (IANO).

f. A forensic backup of the computer system (to include unauthorized systems) will be performed by the DOIM to preserve files which will be provided to the Staff Judge Advocate for legal review to determine if disciplinary action is warranted.

g. If authorized or unauthorized privately owned or Employee Owned Information Systems (EOISs) are found connected to the FSH network and have un-authorized, unlicensed, malicious code or are participating in un-authorized activity, the system will be detained by government IA personnel and assessed for the presences of unauthorized sensitive information. If IA determines the system contains sensitive government information, the system will be sanitized to ensure all information is removed.

h. Organizations whose computers require sanitizing, may be required to incur the cost of returning the computer to working condition.

5. The point of contact is Mr. Jack D. Poland, Director of Information Management, 221-1300/5281, or email address jack.poland1@us.army.mil.

Russell

RUSSELL J. CZERW
Major General, DC
Commanding

DISTRIBUTION:
A